IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Liqun Chen	) On Appeal to the) Board of Appeals
Patent Application No.: 10/613,522	)
Filed: 07/02/2003	) Group Art Unit: 2136
	) Examiner: Abendin, Shanto
For: " Method and Apparatus For Use in ..."	) Date: April 7, 2008

BRIEF ON APPEAL (Amended)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated September 20, 2007, for the above identified patent application. Appellants submit that the original Appeal Brief was timely filed. This version of the Appeal Brief has been amended in response to the Official Action dated March 5, 2008. Authorization to charge a deposit account for the Appeal Brief fee appears in the original Appeal Brief.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-11 and 19-24 are present in the application. Claims 12-18 and 25-28 have been canceled without prejudice. Claims 1-11 and 19-24 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

Claims 12-17, 25, 27 & 28 have been cancelled after the Final Rejection in order to reduce the matters which need to be addressed in this Appeal Brief. Claim 1 has been amended to add a missing article "a" to claim 1. The amendment should be entered as it narrows the issues which will be considered in this Appeal Brief and since the amendment to claim 1 in no way affects its scope. The Applicant is awaiting notice from the Examiner that the amendment to claim 1 and the canceling claims 12-17, 25, 27 and 28 have been entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

In the description of the invention there are two embodiments. A general embodiment is discussed with reference to Figure 2 from page 9, line 15 to page 13, line 8. This is followed by an example of one specific application of the invention which is discussed with reference to Figure 3 beginning at page 13, line 10 and continuing to page 16, line 18. The references set forth before are with respect to the general embodiment of Figure 2.

The invention described and claimed in the present application relates to a method of enabling a third party (p. 9, ll. 13-18; Fig. 2, element 7) to verify the existence of an association (any type of association) between a first party (p. 9, ll. 13-18; Fig. 2, element 5) and a second party (p. 9, ll. 13-18; Fig. 2, element 6) and involves the second party outputting three verification parameters (X, Y, Z; page 10, l. 5 - p. 11, l. 28) which the third party can use to verify the association. More specifically, the three parameters enable the third party to verify that the second party holds a secret that must have been provided by the first party (it is assumed that this secret would have been provided by the first party to the second party in order to enable the existence of an association between the first and second parties to be proved); this secret is called a "shared secret" (p. 10, l. 10; element s_1Q_{ID}) in claim 1 because it is a secret shared by the first party with the second party, though the first party need not, in fact, keep a copy of the secret. Claim 1 is concerned with what the second party does to generate the three verification parameters while claim 8, for example, is concerned with how the third party uses those verification parameters.

Claim 1 is directed to a method of enabling second party (p. 9, ll. 13-18; Fig. 2, element 6) to prove to a third party (p. 9, ll. 13-18; Fig. 2, element 7) the existence of an association between the second party (p. 9, ll. 13-18; Fig. 2, element 6) and a first party (p. 9, ll. 13-18; Fig. 2, element 5), the first party being associated with a first element (p. 10, l. 1; element P) of a first algebraic group (p. 2, l. 6 to p. 3., l. 16; element G_1), the second party being associated with a second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}), of a second algebraic group (p. 2, l. 6 to p. 3., l. 16, element G_1 or G_0), formed from an identifier string (p. 10, l. 10-20; element ID) of the second party (p. 9, ll. 13-18; Fig. 2, element 6) using a hash function (p. 3, l. 13; element H1), and there being a computable bilinear map (p. 2, l 6 to p. 3, l. 16; element *p*) for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party: receives a shared secret (p. 10, l. 10; element s_1Q_{ID}) provided by the first party as the

product of a first secret (p. 10, ll. 1-2; element s_1) and the second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}); computes first (p. 10, ll. 14, 26; element X formed of the product of s_2 and s_1Q_{ID}), second (p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}) and third (p. 11, l. 28; element Z which is formed as a product of s_2 and P) verification parameters as the product of a second secret (p. 10, l. 3; element s_2) with said shared secret (p. 10, l. 10; element s_1Q_{ID}), the second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}) and the first element (p. 10, l. 1; element P) respectively; and outputs the first (p. 10, ll. 14,26; element X formed as a product of s_2 and s_1Q_{ID}), second (p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}) and third (p. 11, l. 28; element Z which is formed as a product of s_2 and P) verification parameters for use by the third party (p. 9, ll. 13-18; Fig. 2, element 7) in proving the association between the first (p. 9, ll. 13-18; Fig. 2, element 5) and second parties (p. 9, ll. 13-18; Fig. 2, element 6).

To reiterate, claim 1 concerns a "second-party computer entity" (p. 9, ll. 13-18; Fig. 2, element 6) generating and outputting three verification parameters (X, Y, Z; p. 10, l. 5 - p. 11, l. 28) of the following form:

a first verification parameter	computed as the product of the second secret (page 10, l. 3; element s_2) with the shared secret (p. 10, l. 10; element s_1Q_{ID}) ;
a second verification parameter	computed as the product of the second secret (page 10, l. 3; element s_2) with the second element (p. 10, l. 3 - p. 11, l. 20; elements Q or Q_{ID});
a third verification parameter	computed as the product of the second secret (page 10, l. 3; element s_2) with the first element (p. 10, l. 1; element P).

Claim 8 is, as previously mentioned, concerned with how the third party uses the verification parameters and is directed to a method of verifying an association between a first party [p. 9, ll. 13-18; Fig. 2, element 5] associated with a first element [p. 10, l. 1;

element P], of a first algebraic group [p. 2, l. 6 to p. 3., l. 16, element G_1], and a second party [p. 9, ll. 13-18; Fig. 2, element 6] associated with a second element [p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}], of a second algebraic group [p. 2, l. 6 to p. 3., l. 16, element G_1 or G_0], the first and second elements being such that there exists a bilinear mapping p [(p. 2, l 6 to p. 3, l. 16; element p)] for these elements, the method comprising a third-party computer entity [p. 9, ll. 13-18; Fig. 2, element 7] carrying out the following operations:

receiving both data indicative of said first element [p. 10, l. 1; element P], and a first product [s_1P] formed by the first party from a first secret [p. 10, ll. 1-2; element s_1]and the first element [p. 10, l. 1; element P];

receiving in respect of the second party both an identifier string [p. 10, l. 10-20; element ID], and first [p. 10, ll. 14, 26; element X formed of the product of s_2 and $s1Q_{ID}$], second [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}] and third [p. 11, l. 28; element Z which is formed as a product of s_2 and P] verification parameters;

computing the second element [p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}] from the identifier string [p. 10, l. 10-20; element ID] of the second party [p. 9, ll. 13-18; Fig. 2, element 6];

carrying out a first check (p. 10, l. 29):

p(third verification parameter [p. 11, l. 28; element Z which is formed as a product of s_2 and P] , computed second element [p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}])= p(first element [p. 10, l. 1; element P], second verification parameter [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}])

carrying out a second check (p.11, l. 30):

p(first element [p. 10, l. 1; element P], first verification parameter [p. 10, ll. 14, 26; element X formed of the product of s_2 and $s1Q_{ID}$)= p(first product [s_1P], second

verification parameter [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}])

the association between the first and second parties being treated as verified if both checks are passed.

Claim 19 is directed to an apparatus arranged to enable a third party (p. 9, ll. 13-18; Fig. 2, element 7) to verify an association between the apparatus and a first party (p. 9, ll. 13-18; Fig. 2, element 5) that has a first secret (p. 10, ll. 1-2; element s_1) and is associated with a first element (p. 10, l. 1; element P) of a first algebraic group (p. 2, l. 6 to p. 3., l. 16, element G_1), the apparatus being associated with a second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}), of a second algebraic group (p. 2, l. 6 to p. 3., l. 16, element G_2), and the first and second elements being such that there exists a bilinear mapping p (p. 2, l 6 to p. 3, l. 16; element p) for these elements; the apparatus comprising:

a memory for holding a second secret (page 10, l. 3; element s_2) and an identifier string (p. 10, l. 10-20; element ID) associated with the apparatus,

means for forming said second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}) from said identifier string (p. 10, l. 10-20; element ID) using a hash function (p. 3, l. 13; element H1),

means for receiving from the first party a shared secret (p. 10, l. 10; element s_1Q_{ID}) based on said first secret (p. 10, ll. 1-2; element s_1) and said first element (p. 10, l. 1; element P), and for storing this shared secret in the memory,

means for computing first (p. 10, ll. 14, 26; element X formed of the product of s_2 and $s1Q_{ID}$), second (p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}) and third (p. 14, ll. 8-19; element $r \bullet (P)$) verification parameters as the product of the second secret (page 10, l. 3; element s_2) with said shared secret (p. 10, l. 10; element

s_1Q_{ID}), said second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}) and said first element (p. 10, l. 1; element P) respectively, and

means for making available said identifier string (p. 10, l. 10-20; element ID) and said verification parameters to the third party (p. 9, ll. 13-18; Fig. 2, element 7).

Claim 22 is directed to an apparatus for verifying an association between a first party [p. 9, ll. 13-18; Fig. 2, element 5] associated with a first element [p. 10, l. 1; element P], of a first algebraic group [p. 2, l. 6 to p. 3., l. 16, element G_1], and a second party [p. 9, ll. 13-18; Fig. 2, element 6] associated with a second element [p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}], of a second algebraic group [p. 2, l. 6 to p. 3., l. 16, element G_2]; the first and second elements being such that there exists a bilinear mapping $\hat{p}$ [p. 2, l 6 to p. 3, l. 16; element p] for these elements; the apparatus comprising:

means for receiving both data indicative of the first element [p. 10, l. 1; element P], and a first product [s_1P] formed by the first party from a first secret [p. 10, ll. 1-2; element s_1] and the first element [p. 10, l. 1; element P];

means for receiving in respect of the second party both an identifier string [p. 10, l. 10-20; element ID], and first [p. 10, ll. 14, 26; element X formed of the product of s_2 and $s1Q_{ID}$], second [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}] and third [p. 14, ll. 8-19; element r•(P)] verification parameters;

means for computing the second element (p. 10, l. 3 - p. 11, l. 20; elements Q and/or Q_{ID}) from the identifier string (p. 10, l. 10-20; element ID) of the second party using a hash function (p. 3, l. 13; element H1);

means for carrying out a first check:

$\hat{p}$(third verification parameter [p. 14, ll. 8-19; element r•(P)], computed second element [page 10, l. 3 to p. 11, l. 20; Q or Q_{ID}])= $\hat{p}$(first element [p. 10, l. 1;

element P], second verification parameter [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}])

means for carrying out a second check:

p(first element [p. 10, l. 1; element P], first verification parameter [p. 10, ll. 14, 26; element X formed of the product of s_2 and s_1Q_{ID}])= p(first product [s_1P], second verification parameter [p. 10, ll. 5,26; element Y which is formed as a product of s_2 and Q_{ID}]);

means responsive to both checks being passed, to confirm that there exists an association between the first and second parties.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1 - 7 and 19 - 21 are patentable under 35 U.S.C. 103(a) in view of Gentry, U.S. Patent Pub. No. 2003/0182554, (hereinafter "Gentry '554"), in view of Boneh, U.S. Patent Pub. No. 2003/001785, (hereinafter "Boneh") further in view of Gentry, U.S. Patent Pub. No. 2003/0179855, (hereinafter "Gentry '885")?

Issue 2: Whether Claims 8 - 11 and 22 - 24 are patentable under 35 U.S.C. 103(a) in view of Gentry, U.S. Patent Pub. No. 2003/0182554, (hereinafter "Gentry '554"), in view of Boneh, U.S. Patent Pub. No. 2003/001785, (hereinafter "Boneh") further in view of Gentry, U.S. Patent Pub. No. 2003/0179855, (hereinafter "Gentry '885")?

ARGUMENT

Issue 1: Whether Claims 1 - 7 and 19 - 21 are patentable under 35 U.S.C. 103(a) in view of Gentry, U.S. Patent Pub. No. 2003/0182554, (hereinafter "Gentry '554"), in view of Boneh, U.S. Patent Pub. No. 2003/001785, (hereinafter "Boneh") further in view of Gentry, U.S. Patent Pub. No. 2003/0179855, (hereinafter "Gentry '885")?

In the final Office Action of September 20, 2007, the Examiner rejects Claims 1 - 7 and 19 - 21 under 35 U.S.C. 103(a) as being unpatentable in view of Gentry, U.S. Patent Pub. No. 2003/0182554, (hereinafter "Gentry '554"), and further in view of Boneh, U.S. Patent Pub. No. 2003/001785, (hereinafter "Boneh") and still further in view of Gentry, U.S. Patent Pub. No. 2003/0179855, (hereinafter "Gentry '885"). Appellant respectfully disagrees.

Prior to making issuing this final rejection, the Examiner rejected these claims as being fully anticipated by Gentry '554 to which the applicant responded by asserting, *inter alia*, that Gentry '554 does not teach the computation of quantities having the form of the three verification parameters mentioned in each of the three independent claims. In the final rejection, the Examiner asserts that Gentry '554 does indeed teach teach the computation of quantities having the form of the three verification parameters mentioned in each of the three independent claims and uses the two other references to address other language of the claims. See page 5 of the official action.

<u>The teachings of Gentry '554</u>

So before considering whether or not it is obvious to combine the teachings of the three cited references, the Applicant wishes to consider the teachings of Gentry '554 alone to see whether or not it teaches what the Examiner says it teaches. A before going into detail into Gentry '554 in detail, it is note that the examiner has referenced passages from Gentry relating to his Figure 1 embodiment. In fact, this embodiment appears to be

a generalized statement of the two embodiments shown in Figures 4 and 5. Thus, in [0024] which relates to the Figure 1 embodiment, reference is made to:

> "a first intermediate shared secret component that is determined using a "first random secret and a system parameter"
>
> and to
>
> "a second intermediate shared secret component that is determined using a "second random secret and a system parameter"

Details of the make-up of the intermediate shared secret components are not given in respect of the Figure 1 embodiment but only in relation to the embodiments of Figures 4 and 5. The differences between Gentry and the Applicant's claims can, in fact, be more easily appreciated by looking at a specific example of Gentry and Applicant has concentrated below on the Figure 5 embodiment which is believed to be closer to the present claims than the embodiment of Figure 4.

As done in the present disclosure, Gentry '554's technology is based on the use of pairings (Weil or Tate).

Gentry '554 discloses a Private Key Generator (PKG) that has a secret **s** which it uses to supply two entities A and B with respective secrets $\mathbf{S_A}$ (= $\mathbf{sP_A}$), $\mathbf{S_B}$ (= $\mathbf{sP_B}$) where $\mathbf{P_A}$ and $\mathbf{P_B}$ are public elements formed from the identities of the entities A and B respectively – see [0022] of Gentry '554.

The two entities A and B can now, without more ado, form a **non-interactive shared secret** S_{AB} by using bilinear mapping as is explained at line 14 of paragraph 0022 of Gentry '554.

The entities A and B also form an **interactive shared secret** by the exchange of intermediate shared secret components. Thus for the Figure 5 embodiment, entity A which has a secret **a**, passes **aP** to entity B, whereas entity B, which has a secret **b**, passes **bP** to entity A; **P** is a public element. Both entities can now form **abP**. This is described in paragraph 0033 of Gentry '554.

The entities now go on to form a common symmetric key using at least the interactive shared secret. The formation of the symmetric key seems to be the purpose of the Gentry '554 arrangement, the symmetric key being used to secure communication between the entities. See paragraph 0002 of Gentry '554.

Patentable Differences between Gentry 554 and Claims 1 and 19

In the present Action the Examiner has had another go at arguing that Gentry '554 discloses the computation of three verification parameters as set out in claim 1 (and in claim 19); thus quoting from page 5 of the Action:

> "compute first ([0033]); interactive shared secret), second ([0024]; second intermediate shared secret component) and third (first intermediate shared secret component) verification parameters as the product of a second secret with the said shared secret ([0022]-[0024]); non-interactive shared secret), the second element and the first element ([0024]-[0025]; first and second random secret) respectively."

The detail in the above-quoted passage should have made it a relatively straightforward task to show that the examiner has still utterly failed to demonstrate that Gentry 554 discloses verification parameters of the form set out in claim 1.

Unfortunately, the quoted passage from the Official Action is woefully inconsistent with itself and the disclosure of Gentry 554 (see Applicant's Responses below). So far as the quoted passage can be understood, the Examiner appears to say, using the Gentry Figure 5 symbols as described in paragraph 0033 for illustration, that:

> the first verification parameter
>
> is the interactive shared secret **abP**;
>
> is computed as the product of a second secret with the non-interactive shared secret $\mathbf{S_{AB}}$

Applicant's Response: Note that the interactive shared secret is not disclosed in Gentry '554 as being generated as the product of a second secret and the non-interactive shared secret $\mathbf{S_{AB}}$ but as the product of a secret **a/b** held by one entity A/B and an intermediate shared secret component **bP/aP** supplied by the other entity B/A (see paragraph 0033 of Gentry '554). Given that **a** and **b**

are independently generated random secrets and that the determination of S_{AB} as a bilinear mapping (see paragraph 0022) involves a further random secret **s** as part of S_A or S_B, it is simply not understood how any product involving S_{AB} could possibly generate the interactive shared secret **abP.**

the second verification parameter
is the second intermediate shared secret component **bP**;
is computed as the product of a second secret with the first random **a**

Applicant's Response: Note that paragraph 0033 references the first random secret as **a** and the second intermediate shared secret component as **bP;** obviously, if the second intermediate shared secret component is computed as indicated by the Examiner, the first random secret **a** would be a factor of the second intermediate shared secret component **bP** - it therefore it appears that the Examiner has mixed up the first and second random secrets **a** and **b**.

the third verification parameter
is the first intermediate shared secret **aP;**
is computed as the product of a second secret with the second random secret **b**

Applicant's Response: Note that paragraph 0033 references the second random secret as **b** and the first intermediate shared secret component as **aP;** obviously, if the second intermediate shared secret component is computed as indicated by the examiner, the second random secret **b** would be a factor of the second intermediate shared secret component **aP** - it therefore it appears that the Examiner has apparently mixed up the first and second random secrets **a** and **b**.

So it seems to Applicant, that due to the problems noted above regarding how the Examiner has described the computation of the quantities equated to the verification parameters of claim 1, Applicant can only sensibly comment on why the indicated quantities cannot possibly be equated to the verification parameters of claim 1.

The examiner asserts that:

the first verification parameter	is	the interactive shared secret **abP**;
the second verification parameter	is	the second intermediate shared secret component **bP**;

the third verification parameter is the first intermediate shared secret component **aP;**

Claim 1 requires that:

"first, second and third verification parameters [are computed] as the product of a second secret with said shared secret, the second element and the first element respectively"

Claim 1 requires:

"means for computing first, second and third verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively"

Claim 1 also requires that the verification parameters are all generated and output by the same entity, namely the "second-party computer entity"

First Distinction: As already noted, the "second secret" of claim 1 is a secret of the "second-party computing entity", that is, the entity doing the computation of all three verification parameters. The "second secret" is required by claim 1 to be a factor of all three verification parameters - the only common factor of the quantities of Gentry 554 identified by the examiner as the verification parameters is the quantity **P**. This quantity **P** is the generator of the first group G (see paragraph 0020) and is public (see paragraph 0033) where P is described as " a public parameter from the first cyclic group G"). P would actually be published by the third-party private key generator PKG.

Clearly, the public generator **P** cannot be equated to a secret held by the entity computing the verification parameters. If the second secret of claim 1 was, in fact, public, the verification parameters would be worthless.

Second Distinction: The second and first intermediate shared secret components that according to the examiner form the first and second verification parameters respectively of claim 1, can only be computed by the distinct Gentry entities **B** and **A** respectively as only entity **B** knows **b** needed to compute the second intermediate shared secret component **bP** and only entity **A** knows **a** needed to compute the first

intermediate shared secret component **aP.** However, claim 1 requires all three verification parameters to be computed by the same entity.

Third Distinction: The second verification parameter of claim 1 is computed as the product of the second secret with the 'second element' where the latter is an element of a second algebraic group and is formed from a public identifier string ("ID") of the second party using a hash function. The Gentry equivalent to the 'second element' of claim 1 is either $\mathbf{P_A}$ or $\mathbf{P_B}$ (see [0022]) depending on whether entity A or B of Gentry is considered by the examiner to correspond to the "second-party computer entity" of claim 1 (this is not made clear). The only quantities in Gentry 554 that are formed as the product of a secret with $\mathbf{P_A}$ or $\mathbf{P_B}$ (and are thus candidates for the second verification parameter) are $\mathbf{S_A}$ (=sP_A) and $\mathbf{S_B}$ (= sP_B) – again, see [0022]. However, neither $\mathbf{S_A}$ nor $\mathbf{S_B}$ can be the second verification parameter because:

- $\mathbf{S_A}$ and $\mathbf{S_B}$ are the private keys respectively of entity A and entity B (see [0022]) – these private keys are kept secret by their respective entities A and B and are not output by these entities as required by claim 1; and
- only the PKG of Gentry '554 can compute $\mathbf{S_A}$ or $\mathbf{S_B}$ as it requires knowledge of the secret **s** which is only known to the PKG (see [0022]). However, the PKG of Gentry 554 is clearly not the "second-party computer entity" of claim 1, not least because it does not receive a shared secret from another entity as is required of the "second-party computer entity" of claim 1.

Gentry '554 does not meet all of the limitations of independent claims 1 and 19 which the Examiner asserts it does meet.

For the reasons stated, it is clear that Gentry '554 does not anticipate the limitations of claims 1 and 19 with respect to the computation of the verification parameters of claims 1 and 19. Furthermore, the major mismatch between the quantities

computed in Gentry '554 and the verification parameters recited by claim 1 is not addressed by asserted combination with the disclosures of the Boneh and the Gentry 885. Of course, the Examiner made no argument to this effect, erroneously believing that Gentry '554 does disclose computation of the verification parameters recited by claim 1.

As indicated above, the Examiner does not rely on Gentry '554 alone, but also cites Boneh and Gentry '885 against claims 1 - 7 and 19 - 21.

While the Examiner insists that Gentry '554 teaches how to compute the three recited verification parameters, the Examiner agrees that Gentry '554 does not provide for their "use by the third party in proving the association between the first and second parties". See page 5 of the Official Action.

Now one would think that if Gentry '554 really taught the three verification parameters, as the Examiner insists, that Gentry '554 would also disclose how to use them. But that does not seem to be the case.

So, the Examiner turns to Boneh and seemingly asserts that that because Boneh allegedly teaches authentication based on three indicia (parameter, master key and ID) that it would then be obvious to modify Gentry '554 in terms of the parameters which the Examiner tries to identify. That is a mere conclusory statement. The only nexus appears to be the number three!

The Examiner next relies on Gentry '885 for apparently the trying to make the same connection based on the number three that he does when relying on Boneh, but with even less analysis.

On page 6 of the Final Rejection the Examiner asserts that the motivation to combine the three citations is to "provide a [sic] alternative third party authentication". Why do that? The Examiner seems to suggest that having multiple authentication schemes would be a good idea. Why is that so? What happens when multiple authentications schemes disagree? Do not such systems really have a single

authentication scheme in order to prevent such split outcomes? The Examiner is speculating here and has cited nothing to support this contention.

Moreover, exactly how is the Gentry '554 reference supposed to be modified based on Boneh and/or Gentry '885, especially considering how the Applicant believes that the Examiner has misconstrued Gentry '554.

The Examiner has not provided a reasonable rationale for combining the teachings of Gentry '554 & Boneh and/or Gentry '885

Of course, 35 U.S.C. § 103 "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The Court stated that obvious analysis "should be made explicit." Id. at 1740-41, citing *In re Kahn*, 441 F.3d 977,988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). For the reasons stated above, the Examiner has failed to provide the required articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

Conclusions as to claims 1-7 and 19-21

For the reasons stated above, the Examiner has failed to provide the required articulated rational for combining the prior art references in the manner done in the Final Rejection. And even if the Examiner could overcome this hurdle,

the proffered combination does not meet each and every limitation of the rejected independent claims 1 and 19 for the reason stated above.

Issue 2: Whether Claims 8 - 11 and 22 - 24 are patentable under 35 U.S.C. 103(a) in view of Gentry, U.S. Patent Pub. No. 2003/0182554, (hereinafter "Gentry '554"), in view of Boneh, U.S. Patent Pub. No. 2003/001785, (hereinafter "Boneh") further in view of Gentry, U.S. Patent Pub. No. 2003/0179855, (hereinafter "Gentry '885")?

Gentry '554 is discussed above with respect to the rejection of claims 1 - 7 and 19 - 21 above .

Patentable Differences between Gentry '554 and Independent Claims 8 and 22

Claim 8 concerns the operations carried out by the third party (or rather a third-party computer entity) in using the verification parameters to verify the existence of an association between the first and second parties. In claim 22 a third party is not specifically mentioned, but the apparatus used is claimed. Note that the make-up of the verification parameters is not specified in claims 8 and 22 (the third party or third party apparatus has no knowledge of this) and so the distinctions discussed above in respect of claim 1 are not be used in respect of independent claims 8 and 22.

However, claims 8 and 22 specify the carrying out of first and second checks each taking the form of a comparison of two different bilinear mappings – the bilinear mapping function is indicated in claim 8 by use of the symbol $\hat{p}$, this symbol having been introduced at line 8, page 2 of the specification as:

"a computable bilinear map $\hat{p}$, for example, a Tate pairing t or Weil pairing $\hat{e}$"

In Gentry each entity A and B uses a bilinear map to form the non-interactive shared secret S_{AB} – see paragraph 0022. This is apparently the only described use of

bilinear mappings in Gentry. The Examiner has pointed to no disclosure of any check involving the comparison of two different bilinear mappings. The closest Gentry comes is in a process in which entity A may seek to prove to entity B that entity A knows the non-interactive shared secret S_{AB} by "generating a MAC for the first intermediate shared secret component using the non-interactive shared secret as the key and communicating this first MAC to the second entity" (see paragraphs 0030 and 0034) - on receiving the MAC value the second entity B can compare this value with a value it has generated in the same manner. This comparison is not the same as comparing two different bilinear mappings as is required by each of the first and second checks of claims 8 and 22. Thus Gentry does not anticipate claims 8 - 11 and 22 - 24.

On page 7 of the Final Rejection, in rejecting claim 8, the examiner refers to paragraphs 0028 - 0034, and claims 11, 18, 19 of Gentry '554:

> **Paragraph [0028]** describes forming a MAC of a message using the symmetric key as the key of a keyed hash over the message. The symmetric key may according to line 5, [0034] have been formed using the non-interactive shared secret S_{AB} but paragraph [0028] certainly does not disclose a check involving comparing two different bilinear mappings.
>
> **Paragraph [0029]-[0031]** describe the Figure 4 embodiment and the only relevant part appears to be step 416 concerning each entity confirming that the other knows the non-interactive shared secret - [0030] describes this in more detail as already explained above.
>
> **Paragraph [0032]-[0034]** describes the Figure 5 embodiment and the only relevant part appears to be step 516 concerning each entity confirming that the other knows the non-interactive shared secret - [0034] describes this in more detail as already explained above.

Gentry's Claim 11 is directed to the process by which each entity confirms that the other entity knows the non-interactive shared secret and adds nothing over [0028]-[0034].

Gentry's Claims 18 and 19 make no mention at all of bilinear mappings.

The cited passages of Boneh '554 clearly do not anticipate the first and second check limitations of either independent claim 8 or 22, and thus their dependent claims are similarly not anticipated.

Likewise, none of the passages referenced by the examiner in Boneh and Gentry '885 discloses effecting a verification by carrying out of first and second checks each taking the form of a comparison of two different bilinear mappings. Indeed, the passages referred to by the Examiner in Boneh do not mention comparing bilinear mappings. In Gentry 885, Figure 9, paragraph 0144 and claim 61 all concern a signature verification process in which both sides of a comparison operation include at least one bilinear mapping; however, the mappings are not the same as set out in independent claims 8 and 22 and there is only a single comparison, not two as required by these two claims (and their dependent claims).

Clearly, neither Boneh or Gentry '885 fill in the gaps left by Gentry '554.

The Examiner agrees that Gentry '554 fails to disclose "a third party computer entity carrying out the above [two] checking operations". See page 7 of the Official Action.

Now one would think that if Gentry '554 really taught the first and second checks using *inter alia* the three verification parameters, as the Examiner insists at the top of page 7 of the Final ejection, that Gentry '554 would also disclose what do do with the alleged first and second checks. But that does not seem to be the case. So the Examiner refers the applicant to Boneh and seemingly asserts that that because Boneh

allegedly teaches authentication based on two checks (a point with which the applicant disagrees for the reasons already stated) that it would then be obvious to modify Gentry '554 in terms of the making use of the two checks which the Examiner tries to identify. That is a mere conclusory statement. The only nexus appears to be the number two in this case. Confusingly, the Examiner again mentions towards the middle of page 7 authentication based on parameter, master key and ID, which was his justification for the three verification parameters when rejecting claim 1.

The Examiner next cites Gentry '885 for apparently the trying to make the same connection based on three alleged verification parameters, as he did when rejecting claim 1, but the nexus of this assertion to the admittedly missing features of the independent claims is something which the Examiner does not bother to explain.

The Examiner never explains why or how on would modify Gentry '554 based on the teachings of Boneh or Gentry '885. Rather the Examiner tries to use the language of the claims as the nexus, reading a limitation from a claim on some missing feature in Gentry '554 and then trying to read the same limitation on a feature in Boneh and/or Gentry '885 which apparently has little or nothing to do with the missing feature and then just assumes that it would be obvious to combine the features since that it was happens in applicant's claims. This is mere conclusory reasoning. The Examiner has not provided articulated reasoning with some rational underpinnings as to why a person of ordinary skilled would be motivated to modify Gentry '554 in some specific way based on either Boneh or Gentry '885.

The Examiner has not provided a reasonable rationale for combining the teachings of Gentry '554 & Boneh and/or Gentry '885

Of course, 35 U.S.C. § 103 "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The Court stated that obvious analysis "should be made explicit." Id. at 1740-41, citing *In re Kahn*, 441 F.3d 977,988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). For the reasons stated above, the Examiner has failed to provide the required articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

Conclusions as to claims 8-11 and 22-24

For the reasons stated above, the Examiner has failed to provide the required articulated rational for combining the prior art references in the manner done in the Final Rejection. And even if the Examiner could overcome this hurdle, the proffered combination does not meet each and every limitation of the rejected independent claims 8 and 22 for the reasons stated above.

* * *

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this paper (and any enclosure referred to in this paper) is being transmitted electronically to the United States Patent and Trademark Office on

April 7, 2008
(Date of Transmission)

Stacey Dawson
(Name of Person Transmitting)

/Stacey Dawson/
(Signature)

April 7, 2008
(Date)

Respectfully submitted,

/Richard P. Berg/

Richard Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Encls:
Claims Appendix;
Evidence Appendix;
Related Proceedings Appendix;

1. A method of enabling second party to prove to a third party the existence of an association between the second party and a first party, the first party being associated with a first element of a first algebraic group, the second party being associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

receives a shared secret provided by the first party as the product of a first secret and the second element;

computes first, second and third verification parameters as the product of a second secret with said shared secret, the second element and the first element respectively; and

outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

2. A method according to claim 1, wherein the second-party computer entity generates a further shared secret from the second secret and an identifier string of a fourth party, the second party outputting this further shared secret to the fourth party for use by the latter as the private key of a public/ private key pair the public key of which is formed by the identifier string of the fourth party.

3. A method according to claim 1, wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities.

4. A method according to claim 1, wherein the first and second algebraic groups are the same.

5. A method according to claim 1, wherein the first and second elements are points on the same elliptic curve.

6. A method of verifying an association between the first and second parties of claim 1 by using a function p providing said bilinear map; the method comprising a third-party computer entity carrying out the following operations using the verification parameters of claim 1:

computing the second element from the identifier string of the second party;

carrying out a first check:

p(third verification parameter, computed second element) = p(first element, second verification parameter)

carrying out a second check:

p(first element, first verification parameter) = p(first product, second verification parameter) where said first product is a public parameter provided by the first party and corresponds to the product of the first secret and the first element;

the association between the first and second parties being treated as verified if both checks are passed.

7. A method according to claim 6, wherein said bilinear mapping function is based on a Tate or Weil pairing.

8. A method of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, the first and second elements being such that there exists a bilinear mapping p for these elements, the method comprising a third-party computer entity carrying out the following operations:

receiving both data indicative of said first element, and a first product formed by the first party from a first secret and the first element;

receiving in respect of the second party both an identifier string, and first, second and third verification parameters;

computing the second element from the identifier string of the second party;

carrying out a first check:

p(third verification parameter, computed second element)= p(first element, second verification parameter)

carrying out a second check:

p(first element, first verification parameter)= p(first product, second verification parameter)

the association between the first and second parties being treated as verified if both checks are passed.

9. A method according to claim 8, wherein said bilinear mapping function is based on a Tate or Weil pairing.

10. A method according to claim 8, wherein the first and second algebraic groups are the same.

11. A method according to claim 8, wherein the first and second elements are points on the same elliptic curve.

12 - 18. (Cancelled)

19. Apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping *p* for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus,

means for forming said second element from said identifier string using a hash function,

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory,

means for computing first, second and third verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively, and

means for making available said identifier string and said verification parameters to the third party.

20. Apparatus according to claim 19, wherein the first and second algebraic groups are the same.

21. A method according to claim 19, wherein the first and second elements are points on the same elliptic curve.

22. Apparatus for verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

means for receiving both data indicative of the first element, and a first product formed by the first party from a first secret and the first element;

means for receiving in respect of the second party both an identifier string, and first, second and third verification parameters;

means for computing the second element from the identifier string of the second party using a hash function;

means for carrying out a first check:

p(third verification parameter, computed second element) = p(first element, second verification parameter);

means for carrying out a second check:

p(first element, first verification parameter) = p(first product, second verification parameter);

means responsive to both checks being passed, to confirm that there exists an association between the first and second parties.

23. Apparatus according to claim 22, wherein said bilinear mapping p is based on a Tate or Weil pairing.

24. Apparatus according to claim 22, wherein the first and second elements are points on the same elliptic curve.

25 - 28. Cancelled.

No evidence is being submitted

No copies of decisions rendered in related proceedings are being submitted.